Is cyberpeace possible?

Christen, Markus ; Bangerter, Endre

DOI: https://doi.org/10.1007/978-3-319-57123-2_13

13

Is Cyberpeace Possible?

Markus Christen and Endre Bangerter

Introduction

In the literature on cyberwar, one finds titles like "Cyber War Will Take Place!"[1] or "The Myth of Cyberwar."[2] They are exemplars of a heated debate about a new battlefield enabled by information and communication technology (ICT). This debate is controversial and authors regularly note a lack of precision in key terminology.[3] In addition, it involves powerful stakeholders and substantial financial interests from state actors like the military or companies active in ICT.[4] The key observation is, however, that the debate on cyberwar is pushed by the transformational forces of the digitalization of society, creating both new opportunities and vulnerabilities.[5] The notion

M. Christen (✉)
University of Zurich, Zurich, Switzerland
e-mail: christen@ethik.uzh.ch

E. Bangerter
Bern University of Applied Sciences, Biel, Switzerland
e-mail: endre.bangerter@jdiv.org

F. Demont-Biaggi (ed.), *The Nature of Peace and the Morality of Armed Conflict*,
DOI 10.1007/978-3-319-57123-2_13

of "cyberwar" often serves as an umbrella term for almost all wrongful acts in cyberspace including cybervandalism, cybercrime, espionage through hacking, or cyberterrorism.[6] It even involves the narrative of mass destruction—an "Electronic Pearl Harbor" so to speak, a deadly strike against vital infrastructures of modern countries. Such a narrative framework can be used to justify extreme regulatory measures that diminish privacy and other liberties, or justify major defense contracts for the private computer security sector.[7]

Given these observations, the cyberwar discussion cannot be decoupled from the dependence of modern societies on information technology, where processing of information and even decision-making to some degree is increasingly outsourced to digital technology. Nobody denies that almost every economic sector has been deeply transformed through the use of computers, the Internet, digital sensor technology and robotic applications. Those changes will affect all social spheres of human life to some degree—meaning that ICT involves a momentum of transgression, creates new asymmetries and supports (geographic) unboundedness.

The transgressive momentum results from the fact that digitalizing information processing in all spheres of life compromises or relativizes the boundaries of social spheres (family and friendship, work, politics, education, commercial activity and production, health care, scientific research, etc.) around which human beings organize their social, institutional, legal and moral world. Due to the enhanced reproducibility and transmissibility of data, the traditional separation of those social spheres, each governed by context-relative norms, policies and rules, are threatened when social networks become banks, friends become marketers, or shopkeepers become intelligence officers. This is problematic, as the human environment is structured in social spheres that provide important reference points for human beings. They expect to be treated differently in a family context compared to, for example, in a governmental organization. They accept inequality in treatment in the economic sphere that they would not accept in the health or legal sphere. The interpretation of moral values such as justice or autonomy, and the rules related to these values, differ along these social spheres. For example, if a person discloses personal information in the health sphere for research

purposes, the moral foundation of this choice is to help other people. But if this information is used in a different sphere such as the economic sphere, to tailor offer conditions or to maximize profit of an insurance company, the original intention to disclose this information and thus its contextual integrity is violated.[8] In addition, digitalization in particular in the economic sector often involves asymmetry in the sense that large differences in economic and technological power of the involved players exist—nevertheless, also small players are able to tackle the competition against large players (for example, the erosion of the music industry starting with file-share services like Napster). Finally, digitalization allows for actions unconstrained by geographical borders, which is exemplified by cross-border activities of hacker groups like Anonymous.

What we consider interesting in that respect is the observation that war has similar effects on affected societies with respect to its transgressive nature, asymmetry and unboundedness: First, war affects all social spheres to some degree and involves the potential to overrule the contextualized moral foundation of a social sphere (e.g., shift towards a state-directed economy to allocate resources). Second, modern wars are often asymmetric, i.e., there are significant differences with respect to technological and financial means between the combatant parties. Nevertheless, also a combatant with limited resources is able to resist a powerful force to a substantial degree. Finally, military conflicts can take place in a large and highly diverse array of places.[9] Thus, the disruptive effects of war appear not only in the vicinity of what, conventionally, one would conceive of as likely battle lines.

The way some authors describe cyberwar is in line with these changing notions of war, as we will outline in Sect. "Rise of the Cyberwar Discussion". We therefore suggest that cyberwar not only is enabled through increasing digitalization, but also stands—at least for some exponents in the cyberwar debate—exemplary for an understanding of war that shares some features of the effect of digitalization on the society as a whole. In what follows, we want to argue against the idea that cyberwar engenders radical changes, which concern the very way in which we understand war. Rather, we suggest that the notion of cyberwar involves a definitional vagueness that is hard to avoid and—at the same time—increases the risk of framing all malicious activity

in cyberspace as potentially war-related. To countervail this tendency, we propose increasing the level of cybersecurity in all domains of the digital society that involve certain structural features, such as decreasing complexity and counteracting (to some degree) interoperability of systems. These structural features align with some core demands of those advocating for cyberpeace.

Our chapter is structured as follows: In Sect. "The Insecure Design of Cyberspace", we first outline the insecure design of cyberspace and digital technology as a starting point of our inquiry. In Sect. "Rise of the Cyberwar Discussion", we provide a general description on what people consider examples of cyberwar. In Sect. "Problems of Defining Cyberwar", we outline terminological problems associated with the current definition of cyberwar. In Sect. "Cyberpeace as a System Property", we argue that the definitional vagueness of the notion of cyberwar is hard to avoid and that a shift of the focus on a minimal level of cybersecurity is required—a standpoint that has been emphasized by those promoting cyberpeace, which includes the principle of prioritizing comprehensive self-defense over offense.

The Insecure Design of Cyberspace

We begin our contribution with a review of the technological aspects underlying the cyberwar discussion. We first discuss the fundamental problems that are widely used for explaining why it is seemingly hard to defend IT systems. The following four points are of particular importance:

- *Asymmetry between defense and offense*: The argument is that IT administrators need to be able to defend every single device (e.g., server, end-user laptop, router, printer, etc.) in their network, whereas it is sufficient for the attacker to subvert a single system to access and subvert the network. This is an interesting reversal compared to conventional warfare, where the attacker usually was disadvantaged when striking against fortified defense lines. Additionally, to this asymmetry in the technical domain, there is an asymmetry favoring attackers in the human domain as well. The observation here is that relatively

few skilled attackers are sufficient to carry out an intrusion, whereas it requires far more skilled defenders to protect the networks of the abundant companies and organizations that are potential targets. There are simply not enough security specialists to secure the current IT infrastructures. This is especially a problem for small and middle-sized enterprises for which it is hard to attract specialists and/or who cannot afford appropriate cybersecurity.

- *Complexity of ICT systems*: Current ICT infrastructures are typically built upon numerous hardware and software components, which are in turn connected by various protocols. In fact, typically layers upon layers of software components are deployed on current infrastructures. As a result, it is impossible to deeply understand our current—possibly overly complex—ICT infrastructure. The cybersecurity community unanimously believes that one needs to deeply understand a system to effectively defend it; as a consequence, complex IT infrastructures are very hard to defend.
- *Software is inherently insecure today*: Software is known to contain programming errors (so-called bugs). Some of these bugs are security relevant. These are so-called software *vulnerabilities*. A software vulnerability, for instance in a PDF reader, allows an attacker to execute malicious code on the victim's machine by letting the victim open an accordingly fabricated PDF document containing a so-called *exploit* for the corresponding vulnerability. Software exploits play an important role in the initial compromise of a victim's machine in many attacks. One does not know how to write bug- and vulnerability free, and thus secure, software today.
- *Lack of attribution and consequences for the attacker*: The goal of attribution is to identify the attacker (group or individual) responsible for an attack. Identification can have various meanings, e.g., identification of an individual hacker for the purpose of legal prosecution, or the association of a state-level attacker with a country. If the attacker is careful, attribution is difficult and time consuming, and sometimes impossible. As a consequence, hacktivists, cybercriminals and similar actors only face a low risk to be apprehended and prosecuted, and deterrence against cyberattacks is low. Moreover, it makes it difficult to differentiate between state and non-state attackers.

> Therefore, the distinction between state and non-state-level attackers is often made based on the sophistication of an attack. This can, however, be a fallacy, since if a victim's security stance is weak, state-level attackers will not have to resort to sophisticated attack techniques, but rather commonly used techniques that are equally accessible to non-state actors.

It is unlikely that any of these problems will be fundamentally and thoroughly solved in the near future. Even worse, emerging technical trends such as the Internet of Things[10] will make security problems even worse, since they further increase the aspects of asymmetry and complexity mentioned previously. In a nutshell, all these observations seem thus to suggest that ICT systems are inherently insecure and that the current state of having abundant attacks and breaches is a direct consequence of this inherent insecurity.

While the core problems sketched here are rarely disputed, there is criticism concerning the somewhat fatalist conclusions being drawn from these problems as well as on the overall assessment of the gravity of the problem. Bejitlich,[11] for instance, points out that there are several myths surrounding the nature of cyberattacks. One is that cyberattacks are "fast," that is, once the attacker manages to breach the network he or she will quickly carry out the core actions of the attack, such as information exfiltration, etc. The other is that "defense is dominated by the offense" and that thus defense is a hopeless endeavor (this corresponds to apparent advantages of an attacker based on the asymmetric relation between attack and defense, as discussed earlier). Bejitlich argues that neither is true. In fact, advanced attackers typically operate slowly over periods of weeks or months. This allows them to avoid triggering obvious intrusion alarms by being too noisy, on the one hand, and to carefully explore the victim's network, on the other. He also points out that defense is not hopeless. He cites the attack on the New York Times,[12] whose network was successfully infiltrated by allegedly Chinese attackers who, however, did not manage to get hold of truly critical data. This example illustrates that breaches are not just black or white and that one may experience a loss of security in parts of the network where relatively insensitive data is processed, whereas

critical data can be protected. This observation is in line with best practices, which suggest to compartmentalize networks and data corresponding to their importance. It seems to be the case, however, that many companies and organizations do not yet follow such and other best practices (e.g., security monitoring).[13]

Anderson et al. (2013) state in their study on the costs of cybercrime that the problem of cybercrime attacks is overstated, typically by agents such as vendors and governmental security organizations whose revenue or even justification of existence is based on overestimating the size of the problem—a similar observation to that made by critics of the current cyberwar discussion.

In summary, we believe that getting cybersecurity right is a difficult problem and that there are indeed substantial attacks happening. However, it seems that many victims have not yet reached the state of the art in securing their networks, which in turn facilitates attacks by non-state-level and state-level actors alike. It is clear that attacks by sufficiently skilled and funded actors are under such circumstances very likely to succeed.

Rise of the Cyberwar Discussion

The insecure design of the current ICT infrastructure outlined in the previous section provides the basis of the contemporary cyberwar debate. Although there is no agreement among experts as to which types of cyber incidents count as examples of "cyberwar," some events triggered the debate to a substantial degree—in particular a concentration of events around the years 2007 to 2009. Those include the intrusion into government networks of England, France and Germany (allegedly by the People's Republic of China), an Israeli airstrike against a nuclear reactor in Syria that presumably followed a hack into the air defense system of Syria, or coordinated attacks against the South Korean and US governments and business websites by unknown attackers (North Korea has been suspected).[14]

Of particular relevance for the rise of the cyberwar discussion, however, were the following three events. In April and May 2007,

Estonia—a country that pushed digitalization to a large extent—suffered from a series of Distributed Denial of Service (DDoS) attacks first against government agencies, and then against private sites and servers in the aftermath of the removal of a communist monument from a park in Tallinn. Those attacks succeeded in forcing the government and the largest banks offline for brief periods.[15]

One year later, cyberattacks occurred in Georgia directly coordinated with a physical land, sea and air attack from Russian forces that were supporting separatists in South Ossetia—an autonomous region of Georgia that strived for independence since 1990. Again, DDoS as well as other means were used against government websites, financial and educational institutions, business associations and news media websites including the BBC and CNN—a preparatory cyberattack that may have aided the success of the conventional intervention and occupation.[16] It's important to note that in neither of these cases (Estonia and Georgia) did the cyber strategy address, alter or otherwise remedy or resolve the underlying political conflict.[17]

Finally, starting in 2009, Stuxnet, a cyber-worm, caused damage to centrifuges of Iran's nuclear reactors. The damage was done exclusively to a cascade of centrifuges, illegally obtained and operated in a highly protected site at Natanz, Iran, in explicit violation of the nuclear nonproliferation treaty. Stuxnet—later unofficially disclosed as an US and Israeli operation—was considered to be an example of an "ethical" cyberweapon[18] because its creators had taken pains in designing it to target only Iranian nuclear processing facilities; yet it had spread far beyond intended targets. Although its damage was highly constrained, Stuxnet's quick broad infection was noticed and required upgrades to antivirus software worldwide, incurring a cost to everyone. The worm also provided excellent ideas for new exploits that are already being used, another cost to everyone[19]—all this shows that even careful design to contain the effect of a cyberweapon leads to collateral damage due to the highly interconnected nature of the ICT infrastructure.

Through these examples, cyberwar has been elevated by some authors from a barely mentioned security concern to one of the greatest military dangers in just a few short years. The cyberattacks in, for example, Estonia were certainly not the first of their kind,[20] and their effects on

Estonia's critical information infrastructure were neither serious nor long lasting. Yet the 2007 events in Tallinn "fired the imagination," culminating in opening the *NATO Cooperative Cyber Defense Centre of Excellence* in Tallinn on 14 May 2008.[21] This Center of Excellence also was responsible for creating the "Tallinn Manual on the International Law Applicable to Cyber Warfare," written at the invitation of the Centre by an independent international group of experts. This 3-year effort aimed to examine how extant international legal norms apply to cyberwarfare.

A quantitative look on the literature supports this observation. Generally, the number of academic papers employing cyberwar terminology steadily increased since the late 1990s (relative to all academic papers on cyber topics), whereas in the lay literature a sudden and substantial increase can be observed right after 2007 (Fig. 13.1, see figure

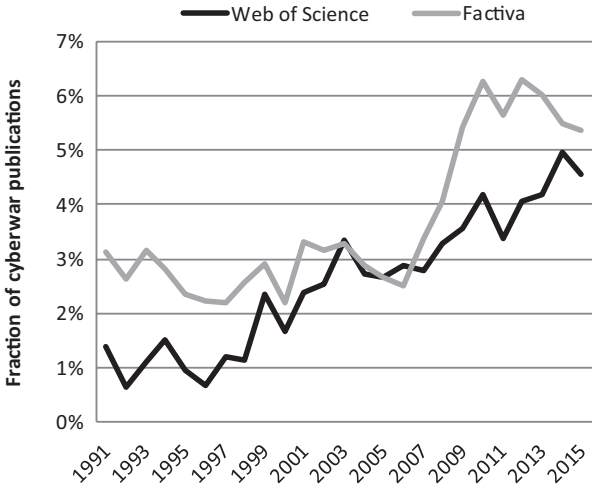

Fig. 13.1 Fraction of "cyberwar publications" compared to all publications containing the terminology of "cyber" in their title or abstract. The search was performed on April 21 2016 in the database *Web of Science* (See https://apps.webofknowledge.com) (scientific literature) and *Factiva* (See https://global.factiva.com) (various types of publications in general media including business sources). The Boolean search expression for "cyberwar papers" was "cyberwar OR (cyber* AND warfare) OR (cyber* AND conflict)," the expression for publications on cyber topics was "cyber*". The time span was 1991 to 2015; we display the relative fraction of cyberwar publications in each database per year

legend for methodological details). This shows that particularly in the popular domain, the events of 2007 to 2009 triggered an intensified interest in cyberwar. For the scientific domain, the steady increase in interest can be traced back to a fundamental reconceptualization in various national security circles around 2000 that digital technology, particularly within the cyber domain, has serious military implications. Thus, cyberspace was conceptualized as an actual environment; an example of this in the United States is the setup of the *Cyber Command*, which unifies all of the existing military cyber activities under a single command.[22]

Problems of Defining Cyberwar

The increasing interest in cyberwar in academic and popular domains does not go along with an increased clarity regarding the definition of the term or with an agreement about which malicious acts in cyberspace should be considered acts of war. Rather, the discussion can be structured along two poles that reflect how the degree of impact and disruptiveness of digitalization is understood.

The representatives of one pole[23] are deeply skeptical towards the proposal that cyberwar is a completely new and independent phenomenon and that it should be understood as war in the traditional sense. Thomas Rid (2013) holds this view. He refers to the definition of war by Carl von Clausewitz according to which aggressive or defensive action must meet three criteria in order to qualify as an act of war. First, acts of war are violent. Second, an act of war is instrumental: physical violence or the threat of force is a means to compel the enemy to accept the attacker's will. Finally, to qualify as an act of war, an attack must have some kind of political goal or intention. Referring to past cases, Rid argues that, so far, a human being has not been injured or hurt as an immediate consequence of a cyberattack and a state never did coerce another state by a cyberattack, which would require disclosing the attacker's identity. But in the contrary, state-sponsored offenders usually don't even take credit for an attack, which makes it difficult to use anonymous attacks for pursuing the political goals of an aggressor.[24]

Gartzke (2013) criticizes that the cyberwar discussion almost exclusively focuses on the *potential* of harm a cyberattack may pose, but the motives and operational logic of perpetrators is not often explored. Specific features of cyberattacks—in particular anonymity, which has been considered to be the most important, and potentially menacing, characteristics of cyberwar[25]—fail to be aligned with strategic goals of war. Although the advantage of anonymity will persist for peripheral forms of warfare on the internet (e.g., for espionage and sabotage), most forms of political conflict encourage disclosing an initiator's identity. On the political level, coercion usually requires attribution—otherwise the "winner" in the conflict is unable to justify the use of resources needed for coercing and he cannot claim the success for his operations.

Even in asymmetric wars that include terrorist acts against civil populations, the direct effects of cyberattacks are likely to be limited. According to Gartzke (2013), it is difficult to see how internet attacks will be able to instill the quality of fear needed to magnify the actions of insurgents. Although no one would be happy when the power goes out or when one's bank account is locked down, attacks of this type cause anger, frustration, even resignation; but not terror as in the case of attacking people with suicide bombers or assault rifles. Furthermore, using cyberweapons requires a certain amount of sophistication, but they are nevertheless deployable usually only for one-off, hard-to-repeat sabotage operations of questionable strategic value that might even prove counterproductive.[26] Taken together, these factors call into question the very idea that computer-assisted attacks will lead to a profoundly new era and "cyberwar" is just a metaphor—analogous to the "war on drugs."

Empirical evidence supports such a critical view on cyberwar. Valeriano and Maness (2014) have collected information on cyber incidents (individual operations launched against a state) and cyber disputes (specific campaigns between two states using cyber tactics during a particular time period that can contain one to several incidents) between rival states in the last decade in order to delineate the patterns of cyber conflict as reflected by evidence on the international level. They found that the actual magnitude and pace of cyber disputes among rivals does not match with popular perception: only

20 of 126 active rivals engaged in activities that can be called cyber conflicts, which the authors define as the use of computational technologies in cyberspace for malevolent and destructive purposes in order to impact, change, or modify diplomatic and military interactions between entities short of war and away from the battlefield. The authors also found that the interactions that were uncovered are limited in terms of magnitude and frequency. Further, most of the cyber disputes that are uncovered are regional in tone.

Representatives of the other pole of the debate[27] has a radically different view on cyberwar. They consider cyberwar a phenomenon that reshapes the concept of war itself.[28] Those representatives consider cyberwar to be an inevitable consequence of digitalization. ICT enables new types of weapons like drones and semi-autonomous robots used to hit ground targets, defuse bombs, and conduct patrolling actions, and ICT creates a new battlefield, the cyber domain. The most striking characteristics of this pole of the debate is that its representatives claim that cyberwar leads to a blurring of the distinction between military and civil society because virtually everybody could become a target.[29] Given that the critical infrastructure of a country increasingly relies on computer control systems that regulate the operations of the infrastructure—e.g., by managing the flow of natural gas through a pipeline, or the production of chemicals—and taking into account that these systems are increasingly connected to other networks, including the Internet, the current mode of organizing society and its economy becomes vulnerable.[30] Along this line, representatives of this pole consider the definitions of war of Rid and others to be too restrictive. They claim that acts of war do not require the use of lethal force and therefore the status of cyberattacks should not be judged on this basis.

The representatives of this pole also take the fact that armed forces increasingly rely on information technology more seriously compared to the representatives of the other pole. The latter certainly admit that the increasing dependence of the military on new technology render them more vulnerable and prone to incidences of potentially crippling cyberattacks. But those who consider cyberwar to redefine how war is waged go beyond that point. They claim, that as digitalization itself is blurring many conceptual boundaries in the real world (see Introduction),

cyberwar exemplifies the blurring of the notion of war: civilians can launch cyberattacks that target both military and civilian infrastructures, cybercriminals can become cyber mercenaries, and the assessment of responsibilities when using semi-autonomous robotic weapons and malware becomes difficult.[31] In summary, representatives of this pole stand for a definitional vagueness of cyberwar, reflecting that war itself has become more difficult to define.

However, for the military practice (and surely also of the theory of cyberwar), such a "definitional openness" of the notion of cyberwar is problematic, as practical issues like adapting the law of armed conflicts to this "fifth domain of war"[32, 33] require a more precise definition. It is thus not surprising that the Tallinn Manual[34] defines a cyberattack rather conservatively, namely as a cyber-operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects. Excluded from this definition are psychological cyber-operations (e.g., blackmailing enemy commanders or undermining their reputation) or cyberespionage. Along these lines, Liff (2012) defines cyberwar as operations that are restricted to computer network operations whose means (not necessarily its indirect effects) are non-physical and that have direct political and/or military objectives—namely, attacks with coercive intent and/or as a means to some strategic and/or brute force end—and computer network defense.

Other authors opt for a broader definition of cyberwar. Lewis (2011), for example, defines cyberwar as the use of cyber techniques to cause damage, destruction, or casualties for political effects by states or political groups. If a cyberwar is defined in such a way, understanding the role of cyberweapons requires asking the same questions as for any other weapons system: what are the range, destructiveness, cost, effect, and political implications of its use? Given what has been witnessed, cyberattacks' physical consequences resemble more those of sabotage acts than those of a strategic weapon or an attack by ground forces. Furthermore, cyberattacks introduce a new dimension in the ability to cause uncertainty, e.g., by manipulating data on which the decisions of the opponents are based.[35]

The Geneva Center for the Democratic Control of Armed Forces (DCAF) adopted an even broader definition of cyberwar in its DCAF

Horizons 2015 Working Paper that includes cybervandalism, cybercrime, and cyberespionage.[36] It defines cyberwar as warlike conduct conducted in virtual space using information, communications technology, and networks, with the intention of disruption or destruction of the enemy's information and communications systems and in this way influencing the decision-making capacity of an opponent's political leadership and armed forces. This definition distinguishes between state-sponsored and non-state-sponsored cyberattacks—a distinction also emphasized by Dipert (2014), who distinguishes between the notion of cyberwar as conducted among nations or nation-like political entities from the notion of a cyberattack by individuals, corporate entities, or other groups of individuals, and further distinguishes both from cyberespionage and from cybertheft of intellectual property. According to Dipert, criminal cyberattacks motivated by financial gains, hacktivist cyberattacks (the subversive use of computers and computer networks to promote a political agenda) or mere vandalism do not count as cyberwar. Regarding attacks conducted as parts of a cyberwar, however, there at least three kinds. First, commanded attacks, ordered or directed by a state's central authority; second, tolerated acts, which are attacks that benefit the host state but that are not initiated and directed by the host state; and third, patriotic acts, which are attacks on behalf of a state but that are not expressly tolerated by the benefited state, perhaps because it does not know of them.[37]

To summarize, all these attempts to define cyberwar show the blurring boundary between acts of cyberwar and other types of malicious activities in cyberspace. This blurring even includes those who actually perform these activities. Cyberattack for hire is a lucrative business for those who have been previously overlooked as merely cybercriminals. As noted by many, including Richard Clarke, former National Coordinator for Security, Infrastructure Protection, and Counterterrorism for the United States, cybercriminals can become rental cyberwarriors.[38] There's even evidence that governments are deliberating cultivating an ecosystem of cybercrime and privateering.[39] All this increases the risk of framing all malicious activity in cyberspace as potentially war-related.

Cyberpeace as a System Property

Our review of the cybersecurity discussion in Sect. "Problems of Defining Cyberwar" reveals that the notion of cyberwar involves a definitional vagueness that is hard to avoid. The reason for that is that the insecure nature of cyberspace outlined in Sect. "The Insecure Design of Cyberspace" actually supports both poles of the cybersecurity debate: Those who support the idea that cyberwar is a new, fundamental threat for modern societies are right when pointing to the fact that the digital infrastructure indeed has vulnerabilities that are hard to overcome—and an increasing dependence on this infrastructure poses new risks. However, the cyberwar sceptics are also right in observing that the nature of these vulnerabilities makes it unlikely that many of the malicious activities in cyberspace conform to warfare as an instrument to reach political goals. They certainly are instruments to support espionage, propaganda and similar activities that are elements of war. Those are instruments where non-attribution is unproblematic or even required, and the advantage of anonymity will persist in some forms of terrestrial competition and conflict. But a cyberwar launched from unidentified sources fails to provide the target with the means to acquiesce and it is in an attacker's interest to "brand" its actions to most effectively elicit concessions from a target.[40] Indeed, even if demands are complied with, an attacker will have difficulty obtaining sustained compliance, given the impossibility of demonstrating future capabilities. Furthermore, when attackers backed by a nation state indeed plan to build strategic war-force in cyberspace, they are confronted with the problem that their own infrastructure is, in principle, in equal danger as that of their opponent, because the digital infrastructure of their own administrations, banks, companies, hospitals, etc. is a comparably easy target.

Given this definitional vagueness of cyberwar and the difficulty to determine which malicious acts in cyberspace actually could count as cyberattacks that constitute a cyberwar, we suggest to change the perspective, namely to focus on a global culture of cybersecurity. This includes various elements such as the availability of warning systems,

built-in redundancies, but also trained behavioral modes like the exploration of areas of cooperation within the stakeholder community as part of a peaceful environment, as well as increased information sharing.[41] Rid (2013) observed that loose talk of cyberwar tends to overhype the offensive potential of cyberattacks such that people who are not cybersecurity practitioners are more likely to ignore the importance (and the potential) of defense measures. The focus on cyberwar also entails the risk that those operating potential (civilian) target ICT systems (e.g., related to the critical infrastructure) believe that military institutions are in charge of dealing with the threat—but companies and individuals need to take responsibility for their own security. Finally, as long as people in organizations practice poor cybersecurity, essentially anybody can successfully carry out an attack; but if anybody can be an attacker, it is impossible to differentiate between attacks done by nation states and simple opportunistic attacks. Thus, a low level of cybersecurity actually increases the difficulty of properly defining cyberwar.

In the near term, a first step would be to consistently apply existing best practices such as reduction of complexity, compartmentalization, or improved monitoring. The first element—reduction of complexity—is indeed hard to attain given that the technology industry is driven by the demand for features, for options, for speed. And each of the products produced by this industry has its own console, its own terminology, its own policies, and its own alerts. Thus, what is needed to reduce complexity are both political (such as introducing liability for insecure software) and practical (e.g., to reduce the diversity of devices used within an organization) measures. The second element involves counteracting interconnectivity of devices at least to some degree. The Director of US National Intelligence recently said during a senate hearing on worldwide threats that interconnected devices could be useful "for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials."[42] In other words, interconnectedness increases the potential of successful cyberattacks as well as their impact (e.g., with respect to the amount of data that can be captured). Likely targets such as critical infrastructures, defense contractors, state-level organizations, etc. should therefore ensure compartmentalization of their

ICT infrastructure, which basically means to divide assets into smaller pieces and secure them separately. For example, this could require not to rely on a single electronic identity and to use different identification markers for different parts of the system. In the mid-term, investments into research and development of defensive technologies are needed, on the one hand, and into skilled cybersecurity specialists, on the other hand.

However, technological and operational advances are unlikely to entirely solve out cybersecurity problems. There are also societal and cultural advancements that will be needed. Interestingly, this focus on the various aspects that entail such a culture of security have been promoted in a strand of the cybersecurity debate that is often neglected, those who opted for the positive side in the war-peace antinomy, namely cyberpeace.[43] The *International Telecommunication Union* proposed five principles for cyberpeace: First, every government should commit itself to giving its people access to communications. Second, every government will commit itself to protecting its people in cyberspace. Third, every country will commit itself not to harbor terrorists/criminals in its own territories. Fourth, every country should commit itself not to be the first to launch a cyberattack on other countries. Fifth, every country must commit itself to collaborate with each other within an international framework of cooperation to ensure that there is peace (understood as the pursuit of possible benefits and positive potential of ICT) in cyberspace.[44] While these principles are obviously rather abstract, they entail a notion of peace that does not only involve the absence of certain violent acts, but implies the prevalence of legal and general moral principles, possibilities and procedures for settlement of conflicts, durability and stability.[45] Before such a state of cyberpeace can be reached, however, a clear focus on an enhanced cybersecurity culture will be needed, which involves slowing down and simplifying the process of digitalization of all spheres of human life.

Notes

1. Stone (2013).
2. Gartzke (2013).
3. Flowers and Zeadally (2014); Lewis (2011); Lucas (2014).
4. Rid (2013).
5. Floridi (2016).
6. Orend (2014).
7. Deibert (2011).
8. Christen, Markus; Blumer, Helene; Hauser, Christian and Huppenbauer, Markus. The ethics of Big Data applications in the consumer sector. In: Braschler, M.; Stadelmann, T.; Stockinger, K. (eds.): *Applied Data Science - Lessons Learned for the Data-Driven Business*. Submitted.
9. Gregory (2011a, b).
10. The Internet of Things (IoT) is loosely speaking the emerging trend to connect appliances and objects of everyday life (e.g., cars, kitchen and household appliances, watches, smart meters, etc.) to the global Internet. IoT dramatically increases the sheer number of networked devices and increases the diversity of devices, resulting in an increase of overall system complexity.
11. Army Cyber Institute (2016).
12. See Perlroth (2013).
13. This claim is based on private communications with practitioners from the IT security community. However, to our knowledge there are no systematic studies to substantiate this claim, not least of all since many incidents are non-public. Yet, as an example consider the Sony hack, which is surrounded by many speculations about potential nation state actors. Public sources (Goodin 2014) point out that the security stance of Sony was in a bad shape.
14. Flowers and Zeadally (2014).
15. Kaiser (2015).
16. Flowers and Zeadally (2014).
17. Lucas (2014).
18. Lucas (2014).
19. Lin et al. (2014).
20. Hancock (1999).
21. Kaiser (2015).
22. Deibert (2011).
23. E.g. Schmitt (2002); Rid (2013).

24. Liff (2012).
25. Deibert (2011).
26. Rid (2013).
27. E.g. Floridi and Taddeo (2014); Stone (2013).
28. Floridi and Taddeo (2014).
29. Taddeo (2012).
30. Flowers and Zeadally (2014).
31. Floridi and Taddeo (2014).
32. On June 14 2016, the NATO state defense ministers have formally recognized cyberspace as a domain of warfare (Barnes 2016).
33. Editorial (2014).
34. Schmitt (2013).
35. Lewis (2011).
36. Schreier (2013).
37. Dipert (2014).
38. In Flowers and Zeadally (2014).
39. Deibert (2011).
40. Gartzke (2013).
41. Wegener (2011).
42. See Ackerman and Thielman (2016).
43. Wegener (2011).
44. Touré (2011).
45. Wegener (2011).

References

Ackerman, Spencer, and Sam Thielman. 2016. US Intelligence Chief: We Might Use the Internet of Things to Spy on You. *The Guardian*, February 9. https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper.

Anderson, Ross, Chris Barton, Rainer Böhme, Richard Clayton, Michel J.G. van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. 2013. Measuring the Cost of Cybercrime. In *The Economics of Information Security and Privacy*, ed. Rainer Böhme, 265–300. Berlin, Heidelberg: Springer.

Army Cyber Institute. 2016. CyberTalks Sept 2015—Thinking Strategically about Digital Security. YouTube video, 21:35. January 21. https://www.youtube.com/watch?v=ICtg7D3sPJw.

Barnes, Julian E. 2016. NATO Recognizes Cyberspace as New Frontier in Defense. *The Wall Street Journal*, June 14. http://www.wsj.com/articles/nato-to-recognize-cyberspace-as-new-frontier-in-defense-1465908566.

Deibert, Ronald. 2011. Tracking the Emerging Arms Race in Cyberspace. *Bulletin of the Atomic Scientists* 67 (1): 1–8.

Dipert, Randall R. 2014. The Future Impact of a Long Period of Limited Cyberwarfare on the Ethics of Warfare. In *The Ethics of Information Warfare*, ed. Luciano Floridi and Mariarosaria Taddeo, 25–37. Berlin, Heidelberg: Springer.

Editorial. 2014. Special Issue on Cybersecurity, Cybercrime, Cyberwar. *Homeland Security & Emergency Management* 11 (4): 459–461.

Floridi, Luciano. 2016. *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*. Oxford: Oxford University Press.

Floridi, Luciano and Mariarosaria Taddeo. 2014. The Ethics of Information Warfare—An Overview. In *The Ethics of Information Warfare*, eds. Luciano Floridi, and Mariarosaria Taddeo, v–xi. Berlin: Springer.

Flowers, Angelyn, and Sherali Zeadally. 2014. Cyberwar: The What, When, Why, and How. *IEEE Technology and Society Magazine* (Fall) 33 (3): 14–21.

Gartzke, Erik. 2013. The Myth of Cyberwar. Bringing War in Cyberspace Back Down to Earth. *International Security* 38 (2): 41–73.

Goodin, Dan. 2014. Sloppy Security Hygiene Made Sony Pictures Ripe for Hacking. *Ars Technica*, December 18. http://arstechnica.com/security/2014/12/sloppy-security-hygiene-made-sony-pictures-ripe-for-hacking/.

Gregory, Derek. 2011a. From a View to a Kill: Drones and Late Modern War. *Theory, Culture and Society* 28 (7–8): 188–215.

———. 2011b. The Everywhere War. *Geographical Journal* 177 (3): 238–250.

Hancock, Bill. 1999. First Official Cyberwar: Kosovo vs. NATO. *Computers & Security* 18: 557–558.

Kaiser, Robert. 2015. The Birth of Cyberwar. *Political Geography* 46: 11–20.

Lewis, James A. 2011. Cyberwar Thresholds and Effects. *IEEE Security & Privacy* (September/October) 9 (5): 23–29.

Liff, Adam P. 2012. Cyberwar: A New Absolute Weapon? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies* 35 (3): 401–428.

Lin, Patrick, Fritz Allhoff, and Keith Abney. 2014. Is Warfare the Right Framefor the Cyber Debate? In *The Ethics of Information Warfare*, ed. Luciano Floridi and Taddeo Mariarosaria, 39–59. Berlin: Springer.

Lucas, George R. 2014. Permissible Preventive Cyberwar: Restricting CyberConffiict to Justified Military Targets. In *The Ethics of Information Warfare*, ed. Luciano Floridi and Mariarosaria Taddeo, 73–83. Berlin: Springer.

Orend, Brian. 2014. Fog in the Fifth Dimension: The Ethics of Cyber-War. In *The Ethics of Information Warfare*, ed. Luciano Floridi and Mariarosaria Taddeo, 3–24. Berlin: Springer.

Perlroth, Nicole. 2013. Hackers in China Attacked *The Times* for Last 4 Months. *New York Times*, Jan 30. http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?_r=0.

Rid, Thomas. 2013. Cyberwar and Peace. *Foreign Affairs* 92 (6): 77–87.

Schmitt, Michael N. 2002. Wired Warfare: Computer Network Attack and Jus in Bello. *International Review of the Red Cross* 84 (8): 346–365.

———. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

Schreier, Fred. 2013. On Cyberwarfare: DCAF Horizons 2015. Working Paper. Geneva: Defense Center for Armed Forces.

Stone, John. 2013. Cyber War Will Take Place! *Journal of Strategic Studies* 36 (1): 101–108.

Taddeo, Mariarosaria. 2012. Information Warfare: A Philosophical Perspective. *Philosophy and Technology* 25: 105–120.

Touré, Hamadoun I., (ed.) 2011. *The Quest for Cyber Peace*. International Telecommunication Union & World Federation of Scientists. https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01–1-2011-PDF-E.pdf.

Valeriano, Brandon, and Ryan C. Maness. 2014. The Dynamics of Cyber Conflict Between Rival Antagonists, 2001–2011. *Journal of Peace Research* 51 (3): 347–360.

Wegener, Henning. 2011. A Concept of Cyber Peace. In *The Quest for Cyber Peace*, ed. Hamadoun I. Touré, 77–85. International Telecommunication Union & World Federation of Scientists.